

**AMENDMENTS TO THE CLAIMS**

**Claim 1 (currently amended):** System for reading a document-(6) comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document-(6) has a predetermined right, which document at least contains a chip-(5) containing biometric data on a holder as well as data with a predetermined relationship to the machine readable holder details in the machine readable zone, and wherein the system comprises:

- a reader-(8) for reading the chip-(5) and for reading the machine-readable holder details in the machine readable zone;
- a memory-(10) containing details with regard to the predetermined right of the holder;
- a biometric feature scanner-(11) arranged to scan a biometric feature of the holder and to generate scanned biometric data;
- a processing unit-(9) that is connected to the reader-(8), the memory-(10) and the biometric feature scanner-(11) and is equipped to:
  - establish the authenticity of the chip, of the biometric data and of the data having the predetermined relationship to the machine readable holder details with the aid of a public key encryption technology;
  - receive the biometric data on the holder from the chip, from the reader-(8);
  - receive the scanned biometric data on the person presenting the document from the biometric feature scanner-(11) and to compare these with the biometric data on the holder from the chip to determine whether the person presenting the document is the holder;
  - receive the machine readable holder details in the machine readable zone via the reader (8), check the predetermined relationship between the holder details and the data having the predetermined relationship to the machine readable holder details and read the predetermined right of the holder from the memory-(10);
  - provide a signal to indicate the predetermined right for the person presenting the document if the chip-(5), the biometric data and the data are authentic, the predetermined

relationship has been established and the person presenting the document is the same as the holder.

**Claim 2 (original):** System according to Claim 1, wherein the document is a travel document.

**Claim 3 (currently amended):** System according to Claim 1, wherein the processing unit-(9) is equipped to compare the holder's details, using a one-way function, with holder's details stored in the memory-(10).

**Claim 4 (original):** System according to Claim 3, wherein the one-way function is a hashing function.

**Claim 5 (currently amended):** Method for reading a document-(6) comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document-(6) has a predetermined right, which document contains at least one chip-(5) containing biometric data on a holder as well as data having a predetermined relationship to the machine readable holder details in the machine readable zone, and wherein the system comprises a reader-(8) for reading the chip-(5) and for reading the machine-readable holder details in the machine readable zone, a memory-(10) containing data on the predetermined right of the holder, a biometric feature scanner-(11) arranged to scan a biometric feature of the holder and to generate scanned biometric data and a processing unit-(9) that is connected to the reader-(8), the memory-(10) and the biometric feature scanner-(11), wherein the method comprises the following operations performed by the processing unit:

- establishment of the authenticity of the chip, of the biometric data and of the data having the predetermined relationship to the machine readable holder details with the aid of a public key encryption technology;
- receipt of the biometric data on the holder from the chip;
- receipt of the scanned biometric data on the person presenting the document and comparison with the biometric data on the holder from the chip to determine whether the person presenting the document is the holder;
- receipt of the machine readable holder details in the machine readable zone, checking of

the specific relationship between the holder details and the data having the predetermined relationship to the machine readable holder details and reading the predetermined right of the holder from the memory-(10);

- provision of a signal to indicate the predetermined right for the person presenting the document if the chip-(5), the biometric data and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

**Claim 6 (currently amended):** Data carrier comprising a computer Computer-program that can be loaded by a system for reading a document-(6) comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document-(6) has a predetermined right, which document contains at least one chip-(5) containing biometric data on a holder as well as data having a predetermined relationship to the machine readable holder details in the machine readable zone, and wherein the system comprises a reader-(8) for reading the chip-(5) and for reading the machine-readable holder details in the machine readable zone, a memory-(10) containing data on the predetermined right of the holder, a biometric feature scanner-(11) arranged to scan a biometric feature of the holder and to generate scanned biometric data and a processing unit-(9) that is connected to the reader-(8), the memory-(10) and the biometric feature scanner-(11), wherein the computer program can provide the system with the following functionality:

- establishment of the authenticity of the chip-(5), of the biometric data and of the data having the predetermined relationship to the machine readable holder details with the aid of a public key encryption technology;
- receipt of the biometric data on the holder from the chip-(5);
- receipt of the scanned biometric data on the person presenting the document and comparison with the biometric data on the holder from the chip to determine whether the person presenting the document is the holder;
- receipt of the machine readable holder details in the machine readable zone, checking of the specific relationship between the holder details and the data having the

predetermined relationship to the machine readable holder details and reading the predetermined right of the holder from the memory-(10);

- provision of a signal to indicate the predetermined right for the person presenting the document if the chip-(5) and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

**Claim 7 (cancelled)**

**Claim 8 (currently amended):** Document comprising a card provided with machine-readable holder details in a machine readable zone and a chip-(5), which chip-(5) is provided with a processing unit-(14) and memory-(16) connected thereto and an input/output unit-(15), wherein the memory-(16) contains biometric data on a holder, as well as data that have a predetermined relationship to the machine readable holder details in the machine readable zone, as well as instructions for making the processing unit carry out the following operations:

- communication with a system according to Claim 1 to enable the authenticity of the chip (5) to be established with the aid of a public key encryption technology;
- transmission of the biometric data on the holder and the data having the predetermined relationship to the machine readable holder details from the memory-(16) to the system.

**Claim 9 (currently amended):** Document according to Claim 8, wherein the document is a travel document-(6).

**Claim 10 (currently amended):** Document according to Claim 9, wherein the chip-(5) is an integral part of the travel document.

**Claim 11 (previously presented):** Document according to Claim 8, wherein the input/output unit is equipped for contact-free communication.

**Claim 12 (currently amended):** Document according to Claim 8, wherein the chip-(5) is equipped as a transponder unit.

**Claim 13 (previously presented):** Document according to Claim 8, wherein the predetermined relationship is based on hashing the holder's details.

**Claims 14-23 (cancelled)**

**Claim 24 (new):** System according to claim 1, wherein the chip comprises a biocertificate containing the biometric data on the holder as well as the data with a predetermined relationship to the machine readable holder details in the machine readable zone.

**Claim 25 (new):** System according to claim 1, wherein the processing unit is equipped to check the predetermined relationship between the machine readable holder details in the machine readable zone and the data with the predetermined relationship to the machine readable holder details by performing a hashing operation to the machine readable holder details in the machine readable zone.